Les compagnies d'assurance devraient-elles partager des informations sur les cyberattaques pour aider à lutter contre les rançongiciels?

Introduction

Avec la montée en puissance des cyberattaques, notamment les rançongiciels, le rôle des compagnies d'assurance en matière de cybersécurité devient crucial. Ces entreprises, confrontées régulièrement à des incidents via les réclamations de leurs clients, détiennent une quantité importante de données sur les menaces numériques. Le partage de ces informations pourrait constituer un levier majeur dans la lutte collective contre ces attaques. Cependant, ce partage doit être encadré pour garantir son efficacité et préserver la confidentialité des parties concernées.

Les bénéfices du partage d'informations sur les cyberattaques

1. Amélioration de la compréhension des cybermenaces

Les compagnies d'assurance disposent de données précieuses sur les types d'attaques, les vulnérabilités exploitées, et les conséquences des rançongiciels.
Partager ces informations permettrait de :

- Identifier plus rapidement les tendances des cyberattaques.
- Améliorer les outils de prévention à destination des entreprises et des autorités.

Association Des Experts en Securite et Sureté - ADESS
4, allée des Augustins 92390 Villeneuve-la-Garenne
contact@adess-france.fr
www.adess-eu.org

2. Renforcement de la prévention

En rendant ces données disponibles de manière anonyme et sécurisée, les assureurs pourraient contribuer à :

- Sensibiliser les entreprises aux risques les plus courants.
- Proposer des solutions adaptées pour réduire les vulnérabilités.

3. Réduction des incitatifs pour les cybercriminels

La transparence sur les cas de paiement de rançons ou les types de protections efficaces pourrait :

- Dissuader les cybercriminels en rendant leurs attaques moins lucratives.
- Encourager les entreprises à adopter des politiques de cybersécurité renforcées.

4. Optimisation des assurances cyber

Le partage d'informations pourrait aider à:

- Affiner les modèles de risques utilisés par les compagnies.
- Offrir des couvertures et primes mieux adaptées aux besoins des entreprises.

5. Favoriser la collaboration intersectorielle

Une coopération entre assureurs, experts en cybersécurité et institutions publiques servirait de:

- Renforcer la capacité à réagir efficacement aux cybermenaces.
- Contribuer à la mise en place d'un écosystème de cybersécurité résilient.

Les précautions nécessaires pour un partage responsable

Pour éviter tout risque lié à ce partage d'informations, il est essentiel de mettre en place un cadre strict qui sont:

-

- **Anonymisation des données**

  S'assurer que les informations partagées ne permettent pas d'identifier les entreprises victimes.

- **Confidentialité commerciale**

  Protéger les données stratégiques des entreprises.

• Respect des cadres légaux: Garantir la conformité aux réglementations comme le Règlement général sur la protection des données (RGPD).

• Coordination encadrée: Favoriser des plateformes sécurisées et des mécanismes collaboratifs validés par les autorités.

Exemples et initiatives en cours

1. Au niveau européen

Le Digital Operational Resilience Act (DORA) impose aux entreprises financières de signaler les cyber incidents et encourage la coopération.

2. En France

a- La CNIL insiste sur la notification des violations de données, dont près de la moitié sont causées par des rançongiciels.

b-Le ministère de l'Économie met en avant des pistes de collaboration pour améliorer la protection des entreprises face aux risques cyber.

3. Au niveau international

Le Sommet de la Counter Ransomware Initiative (CRI) encourage le partage d'informations et la coopération entre pays pour lutter contre les rançongiciels.

Conclusion:

Le partage d'informations sur les cyberattaques par les compagnies d'assurance représente une opportunité de taille pour renforcer la lutte contre les rançongiciels. En collaborant de manière structurée et transparente, les assureurs, les entreprises et les autorités pourraient créer un environnement plus sécurisé.
Néanmoins, cela exige une vigilance accrue pour protéger les données sensibles et garantir que ce partage profite à l'ensemble des parties prenantes.

Références:

1. DORA (Digital Operational Resilience Act) - Assuralia : https://www.assuralia.be/fr/article/.dora-un-defi-majeur-pour-les-compagnies-dassurance

2. Notification des violations de données - CNIL : https://www.cnil.fr/fr/diffusion-de-donnees-piratees-la-suite-dune-cyberattaque-quels-sont-les-risques-et-les-precautions

3. Protection des entreprises contre les risques cyber - Ministère de l'Économie : https://www.economie.gouv.fr/risques-cyber-pistes-protection-entreprises

4. Sommet international sur les rançongiciels (CRI) - ANSSI : https://cyber.gouv.fr/actualites/.sommet-de-la-cri-renforcer-la-cooperation-internationale-contre-les-rancongiciels

Anonyme

Association Des Experts en Securite et Surete - ADESS
4, allée des Augustins 92390 Villeneuve-la-Garenne
contact@adess-france.fr
www.adess-eu.org